so organized that differences of color, *i. e.*, differences in the rapidity of ether vibrations, would present themselves to him somewhat as distances from a fixed plane do to us. His intuition would, in a sense, be closer to the truth than ours. For, he would see at a glance that the differences which we attribute to color are relations of a quantitative rather than of a qualitative nature, an idea at which *we* can arrive only as a consequence of elaborate theories and complicated experiments.

Without asserting such to be the case, we cannot dismiss offhand the possibility that absolute space, if it exists at all, has more than three dimensions, that these additional dimensions do not however present themselves to us as such, but become sensible in a masked form as color, electric charges, etc. There is no logical reason why a mathematical theory of color or of electricity might not be built upon such a basis.

Unless we assume dogmatically that space is exactly as it appears to us because we create it with all of its properties, so that objectively it does not exist at all, and unless we deny, dogmatically, the possibility that some other race of thinking beings might possess a space concept also subjective, but different from ours, there remains only one possible way of saving the proposition that space cannot have more than three dimensions, and that And that would be the trivial method of defining it in that way.

ON THE NUMERICAL FACTORS OF CERTAIN ARITHMETIC FORMS.*

By R. D. CARMICHAEL, Princeton University.

The methods used by Dickson in an article on the cyclotomic function† may be applied with some change so as to obtain a set of more general propositions than those at which he arrives and of such nature that his theorems are the simplest cases of those thus obtained. The object of this paper is to generalize the theorems of Dickson; and his method of proof will be freely employed.

We shall let

$$Q_n(x)=0$$

be the equation whose roots are the primitive nth roots of unity without repetition. Then $Q_n(x)$ is a polynomial in x with integral coefficients, that of the highest power being unity. The degree of the equation is $\phi(n)$, $\phi(n)$ being Euler's function.

*Read before the American Mathematical Society, February 29, 1908.

†The American Mathematical Monthly, Vol. XII, pp. 86—89.

As a permanent notation, set

$$n=p_1^{a_1}\,p_2^{a_2}\ldots p_r^{a_r}$$

where the p's are different primes and the a's are integers. From the theory of the primitive roots of unity, we have*

$$(1)\qquad x^n-1=\Pi\, Q_d(x),$$
$$(2)\qquad x^{n/p_1}-1=\Pi\, Q_\delta\,(x),$$

where d ranges over all the divisors of n, and δ over all the divisors of n/p_1. Dividing equation (1) by equation (2), member for member, we have

$$(3)\qquad x^{n(p_1-1)/p_1}+x^{n(p_1-2)/p_1}+\ldots+x^{n/p_1}+1=\Pi\, Q_c(x),$$

where c ranges over all the divisors of n containing the factor $p_1^{a_1}$. Hence $Q_c(x)$ is a polynomial in x with integral coefficients.

Let β be any integer positive or negative, zero excluded, and α any integer prime to β. (If $\beta=1$, α is any integer whatever.) In (3) replace x by α/β. Multiply both terms of the resulting equation by $\beta^{n(p_1-1)/p_1}$; we have

$$(4)\qquad \alpha^{n(p_1-1)/p_1}+\alpha^{n(p_1-2)/p_1}\,\beta^{n/p_1}+\alpha^{n(p_1-3)/p_1}\,\beta^{2n/p_1}+\ldots$$
$$+\alpha^{n/p_1}\,\beta^{n(p_1-2)/p_1}+\beta^{n(p_1-1)/p_1}$$
$$=\beta^{n(p_1-1)/p_1}\,\Pi\, Q_c(\alpha/\beta).$$

Denote by $Q_c(\alpha,\beta)$ the quantity $\beta^{\phi(c)}Q_c(\alpha/\beta)$. It is evident that $Q_c(\alpha,\beta)$ is a homogeneous polynomial in α, β with integral coefficients. Equation (4) may now take the following form:

$$(5)\qquad \alpha^{n(p_1-1)/p_1}+\alpha^{n(p_1-2)/p_1}\,\beta^{n/p_1}+\ldots+\alpha^{n/p_1}\,\beta^{n(p_1-2)/p_1}+\beta^{n(p_1-1)/p_1}=\Pi\, Q_c(\alpha,\beta).$$

In $x^{n/p_1}-1$ replace x by α/β and multiply by β^{n/p_1}. This gives $\alpha^{n/p_1}-\beta^{n/p_1}$. We are now able to find the highest common factor of $\alpha^{n/p_1}-\beta^{n/p_1}$, and $Q_c(\alpha,\beta)$. To this end divide the first member of (5) by $\alpha^{n/p_1}-\beta^{n/p_1}$. A remainder of $p_1.\beta^{n(p_1-1)/p_1}$ is found. This remainder must contain the greatest common divisor sought. But since α and β are relatively prime $\alpha^{n/p_1}-\beta^{n/p_1}$ is not divisible by β. Therefore 1 or p_1 is the greatest common divisor of $\alpha^{n/p_1}-\beta^{n/p_1}$ and $\Pi Q_c(\alpha,\beta)$, the second member of (5). Therefore only one factor of $\Pi Q_c(\alpha,\beta)$ can contain p_1 if $\alpha^{n/p_1}-\beta^{n/p_1}$ contains p_1^2. Hence we have the following theorem:

*See Bachmann's *Kreistheilung*, especially the third and fifth lectures.

THEOREM I. *When α and β are relatively prime integers, the greatest common divisor of $\alpha^{n/p_1}-\beta^{n/p_1}$ and any $Q_c(\alpha, \beta)$ is 1 or p_1, n and c being defined as before. Also, not more than one of the numbers $Q_c(\alpha, \beta)$ contains the factor p_1 when $\alpha^{n/p_1}-\beta^{n/p_1}$ contains p_1^2.*

Suppose that $\alpha^{n/p_1}-\beta^{n/p_1}$ is divisible by p_1, and set this number equal to kp_1, where k is an integer. Then

$$\alpha^{n/p_1}=\beta^{n/p_1}+kp_1.$$

Substituting this value of α^{n/p_1} in the left member of (5) and combining like powers of β, we have

$$p_1\beta^{n(p_1-1)/p_1}+\tfrac{1}{2}p_1(p_1-1)kp_1\beta^{n(p_1-2)/p_1}+\text{terms in } p_1^2,\ p_1^3,\ \ldots$$

Therefore p_1^2 divides the first member of (5) only when

$$p_1\beta^{n(p_1-1)/p_1}+\tfrac{1}{2}p_1(p_1-1)kp_1\beta^{n(p_1-2)/p_1}\equiv 0 \pmod{p_1^2}.$$

Now p_1 is a factor of $\alpha^{n\div p_1}-\beta^{n\div p_1}$, a number to which β is evidently prime; for α and β are relatively prime integers. Hence β is not divisible by p_1. Then the above congruence reduces to

$$p_1\beta^{n/p_1}+\tfrac{1}{2}p_1(p_1-1)kp_1\equiv 0 \pmod{p_1^2}. \tag{6}$$

It is evident that this does not hold when $p_1>2$. Hence the second member of (5) does not contain p_1^2 when $\alpha^{n\div p_1}-\beta^{n\div p_1}$contains $p_1>2$. Hence

THEOREM II. *When α and β are relatively prime integers and p_1 is an odd prime dividing $\alpha^{n\div p_1}-\beta^{n\div p_1}$, not more than one of the numbers $Q_c(\alpha, \beta)$, c as before, is divisible by p_1, and none of them is divisible by p_1^2.*

Consider the case $p_1=2$ in congruence (6) above. We have

$$2\beta^{n\div 2}+2k\equiv 0 \pmod{4},$$

which reduces to

$$\beta^{n\div 2}+k\equiv 0 \pmod{2}.$$

Hence β and k are both odd or both even. Now the equation $\alpha^{n\div p_1}-\beta^{n\div p_1}=kp_1$ reduces in the present case to

$$\alpha^{n+2}-\beta^{n\div 2}=2k. \tag{7}$$

If k and β are both even, then (7) shows that α is also, contrary to the assumption of α and β relatively prime. Hence k and β are both odd; and therefore by (7) α is also. Moreover it is evident from (7) that of the numbers $\alpha^{n\div 2}$, $\beta^{n\div 2}$ one is congruent to 1 and the other to 3 modulo 4. This requires that $n/2$ shall be odd and that of the numbers α and β one shall be congruent to 1 and the other to 3 modulo 4.

Since $n/2$ is odd it follows that the range of c is over a set of numbers each of which is twice an odd number, unity being included among these odd numbers. u being such an odd number it is evident that $Q_{2u}(\alpha, \beta)$ is equal to or a factor of $\alpha^{u-1}+\alpha^{u-2}\beta+\ldots+\beta^{u-1}$, when $u>1$. But since neither α nor β is even, this last expression contains an odd number of odd terms and is therefore odd. Hence $Q_{2u}(\alpha, \beta)$ is odd when $u>1$. Also, $Q_2(\alpha, \beta)=\alpha+\beta$ and is now divisible by 4; for $\alpha+\beta\equiv 1+3 \pmod 4$. From these considerations we deduce the following proposition:

THEOREM III. *If α and β are relatively prime integers and 2 is a factor of $\alpha^{n/2}-\beta^{n/2}$, then $Q_c(\alpha, \beta)$ is divisible by 2^2 only when $c=2$ and of the numbers α, β one is congruent to* 1 *and the other to* 3 *modulo* 4.

We shall now determine the case in which $Q_c(\alpha, \beta)$ is divisible by p_1.

Set $c=mp_1^{a_1}$, m being an integer >1 and not divisible by p_1. Dickson has shown* that

$$Q_c(x)=Q_n(x^{p_1^{a_1}})\div Q_m(x^{p_1^{a_1-1}}).$$

If in this equation x is replaced by α/β and each function Q is multiplied by that power of β whose index is equal to the degree of the function, there results the following equation:

$$(8)\qquad Q_c(\alpha, \beta)=Q_m(\alpha^{p_1^{a_1}}, \beta^{p_1^{a_1}})\div Q_m(\alpha^{p_1^{a_1-1}}, \beta^{p_1^{a_1-1}}).$$

Now by Fermat's Theorem, $\alpha^{p_1}\equiv\alpha$, $\beta^{p_1}\equiv\beta \pmod{p_1}$. Therefore the second member of (8) is congruent to

$$Q_m(\alpha, \beta)\div Q_m(\alpha, \beta)$$

modulo p_1. Now this quantity is 1 unless $Q_m(\alpha, \beta)\equiv 0 \pmod{p_1}$. Hence $Q_c(\alpha, \beta)\equiv 1 \pmod{p_1}$ unless $Q_m(\alpha, \beta)\equiv 0 \pmod{p_1}$.

Consider the case when $Q_m(\alpha, \beta)\equiv 0 \pmod{p_1}$. Now $Q_m(\alpha, \beta)$ divides algebraically

$$(9)\qquad (\alpha^m-\beta^m)\div(\alpha^{m/q}-\beta^{m/q})=\alpha^{m(q-1)/q}+\alpha^{m(q-2)/q}\beta^{m/q}+\ldots+\beta^{m(q-1)/q},$$

where q is any prime factor of m. If

*THE AMERICAN MATHEMATICAL MONTHLY, Vol. XII, p. 86.

$$(10) \qquad \alpha^{m/q} \equiv \beta^{m/q} \pmod{p_1},$$

the second member of (9) is congruent to $q\,\beta^{m(q-1)/q} \pmod{p_1}$. Then there is some integer k such that

$$kQ_m(\alpha, \beta) \equiv q\,\beta^{m(q-1)/q} \pmod{p_1}.$$

Now q is different from p_1; for it is a factor of m which is prime to p_1. Therefore when (10) holds $Q_m(\alpha, \beta)$ is not divisible by p_1 when β is not so divisible. But if β is divisible by p_1, $Q_m(\alpha, \beta)$ is not congruent to zero modulo p_1; and hence $Q_c(\alpha, \beta) \equiv 1 \pmod{p_1}$.

There is left the case $\alpha^{m/q}$ not congruent to $\beta^{m/q}$ and $Q_m(\alpha, \beta) \equiv 0$ modulo p_1. From the last congruence follows

$$(11) \qquad \alpha^m - \beta^m \equiv 0 \pmod{p_1},$$

for $Q_m(\alpha, \beta)$ is a factor of $\alpha^m - \beta^m$. But since

$$\alpha^{m/q} - \beta^{m/q} \text{ is not} \equiv 0 \pmod{p_1},$$

where q is any prime divisor of m, it follows that m is the least exponent for which congruence (11) holds.

These considerations lead to the following theorem:

THEOREM IV. *If α and β are relatively prime integers and $c=mp_1^{\alpha_1}$, where $m>1$ and not divisible by p_1, then $Q_c(\alpha, \beta)$ is divisible by p_1 if and only if the congruence $\alpha^m \equiv \beta^m$ (mod p_1) holds for m and for no exponent less than m. In all other other* cases *$Q_c(\alpha, \beta) \equiv 1$ (mod p_1).*

If m contains any prime factor greater than p_1, the condition that $\alpha^m \equiv \beta^m \pmod{p_1}$ holds for no exponent less than m is not satisfied; and therefore we have the following corollary:

COROLLARY I. *No one of the prime factors of c except the greatest can divide $Q_c(\alpha, \beta)$. For other prime factors of c we have always $Q_c(\alpha, \beta) \equiv 1$.*

COROLLARY II. *When c contains an odd factor $Q_c(\alpha, \beta)$ is odd, α and β being relatively prime integers.*

If we set $v=p_1^{\alpha_1}$, we may write

$$Q_v(\alpha, \beta) = (\alpha^{p_1^{\alpha_1}} - \beta^{p_1^{\alpha_1}}) \div (\alpha^{p_1^{\alpha_1-1}} - \beta^{p_1^{\alpha_1-1}}) \equiv \frac{\alpha-\beta}{\alpha-\beta} \pmod{p_1}.$$

Hence $Q_v(\alpha, \beta) \equiv 1 \pmod{p_1}$ unless $\alpha \equiv \beta \pmod{p_1}$. In the latter case it is evident that $Q_v(\alpha, \beta) \equiv 0 \pmod{p_1}$. Therefore

THEOREM V. *If α and β are relatively prime integers and $v=p_1^{\alpha_1}$,*

$Q_v(\alpha, \beta) \equiv 0$ *or* 1 (mod p_1) *according as* $\alpha-\beta$ *is or is not congruent to* 0 (*mod* p_1).

Corollary I. *If* $\alpha \equiv \beta$ (*mod* p_1), $\alpha^{p_1^{a_1}}-\beta^{p_1^{a_1}}$ *is divisible bg* $p_1^{a_1+1}$. For,

$$\alpha^{p_1^{a_1}}-\beta^{p_1^{a_1}}=\Pi\, Q_d(\alpha, \beta),$$

where d runs over all the a_1+1 divisors of $p_1^{a_1}$. Each factor of the second member contains p_1.

If p_1 is an odd prime the preceding corollary can be made more exact in view of the last clause in Theorem II:

Corollary II. *If* p_1^r *is the highest power of an odd prime* p_1 *contained in* $\alpha-\beta$, *then* $\alpha^{p_1^{a_1}}-\beta^{p_1^{a_1}}$ *is divisible by* $p_1^{a_1+r}$ *but by no higher power of* p_1.

Combining Corollary II with Theorem IV we readily deduce the following.

Theorem VI. *If* α *and* β *are relatively prime integers and* $\alpha-\beta$ *contains* p_1^r *and no higher power of* p_1, *then* $\alpha^{mp_1^{a_1}}-\beta^{mp_1^{a_1}}$ *contains* $p_1^{a_1+r}$ *and no higher power of* p_1 *m as before being prime to* p_1.

We are now prepared to prove the following theorem:

Theorem VII. *If* α *and* β *are relatively prime integers,* $Q_c(\alpha, \beta)$ *has a prime factor not dividing* $\alpha^s-\beta^s$ $(s<c)$, *except in the cases*

1) $c=2$, $\beta=1$, $\alpha=2^k-1$, *where k is an integer.*

2) $Q_c(\alpha, \beta)=p$, *the greatest prime factor of c, and* $\alpha^{n/p}-\beta^{n/p}\equiv 0$ (mod p).

3) $Q_c(\alpha, \beta)=1$.*

Every prime factor of $Q_c(\alpha, \beta)$ is evidently contained in $\alpha^c-\beta^c$. Now if $\alpha^s-\beta^s$ and $\alpha^c-\beta^c$ contain a common prime factor q, it follows from the congruences

$$\alpha^s\equiv\beta^s,\ \alpha^c\equiv\beta^c \text{ (mod } q)$$

that

$$\alpha^l\equiv\beta^l \text{ (mod } q),$$

where l is the greatest common divisor of s and c. Hence every common prime factor of $\alpha^s-\beta^s$ and $Q_c(\alpha, \beta)$ is contained in some $\alpha^d-\beta^d$ where d is a divisor of n. Now evidently, every $\alpha^d-\beta^d$ is contained in $\alpha^{c/p_i}-\beta^{c\ p_i}$ where for p_i is put the different prime factors of n. By Corollary I to Theorem IV, $Q_c(\alpha, \beta)$ does not contain p unless p is the greatest prime factor of c. Then if $\alpha^{c/p}-\beta^{c/p}$ and $Q_c(\alpha, \beta)$ contain the common factor p, $Q_c(\alpha, \beta)$ does not contain p^2 unless $n=2$, as is seen from Theorems II and III. If $c=2$, $Q_c(\alpha, \beta)=\alpha+\beta$, and this contains a factor different from those of $\alpha-\beta$ unless $\beta=1$, $\alpha=2^k-1$. This accounts for the first exception.

If $n\neq 2$ and $Q_c(\alpha, \beta)$ and $\alpha^{c/p}-\beta^{c/p}$ contain the common factor p,

*The author knows no numerical case for positive β under exception 3) and only one under exception 2); namely, $Q_6(2, 1)=2^2-2+1=3$.

$Q_c(\alpha, \beta)$ does not contain p^2, as we have just seen. But these two numbers contain no other factor in common, as is seen from Theorem I. Hence $Q_c(\alpha, \beta)$ contains a prime not in $\alpha^{c/p}-\beta^{c/p}$ at least in every case for which $Q_c(\alpha, \beta) \neq p$ and also in every case for which $\alpha^{c/p}-\beta^{c/p}$ is not divisible by p, unless $Q_c(\alpha, \beta)=1$.

COROLLARY. *$\alpha^c-\beta^c$ has always a prime factor not dividing $\alpha^s-\beta^s$ $(s<c)$ except in the cases mentioned in Theorem VII.*

NOTE ON THE EXTENSION OF THE EXPONENTIAL THEOREM.

By E. D. ROE, JR., Syracuse University.

In the writer's paper in the June-July number of the MONTHLY, pp. 101-106, it will be observed that the complex roots, infinite in number, arising from the application of an incommensurable exponent are tacitly neglected, only the single real root being used. In fact this is the only root that is of much practical value. It is the only root that is usually considered in the extension of the binomial theorem for the expansion of $(1+x)^n$, even for a commensurable fractional exponent. The finite number of complex roots can be easily expressed if wanted. But when the exponent is incommensurable the number of complex roots becomes infinite and the complex roots become indeterminate.

In both cases, vis., of the binomial theorem, and the exponential theorem, which depends on the binomial theorem, the developments already obtained would have to be multiplied by $\cos \varphi+i \sin \varphi$, to obtain the complete development, where φ admits the value of zero, and has besides an infinite number of values which are indeterminate, when the exponent is incommensurable. All the values would have the same modulus.

These facts are so obvious that it will doubtless appear superfluous to many readers to call attention to them; yet for others it may not be amiss to do so.